

Calendar No. 489

106TH CONGRESS
2D SESSION

S. 1993

[Report No. 106-259]

A BILL

To reform Government information security by
strengthening information security practices
throughout the Federal Government.

APRIL 10, 2000

Reported with an amendment

Calendar No. 489

106TH CONGRESS
2D SESSION**S. 1993****[Report No. 106–259]**

To reform Government information security by strengthening information security practices throughout the Federal Government.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 19, 1999

Mr. THOMPSON (for himself, Mr. LIEBERMAN, Mr. ABRAHAM, Mr. VOINOVICH, Mr. AKAKA, Mr. CLELAND, Ms. COLLINS, Mr. STEVENS, and Mr. HELMS) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

APRIL 10, 2000

Reported by Mr. THOMPSON, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

A BILL

To reform Government information security by strengthening information security practices throughout the Federal Government.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Government Informa-
3 tion Security Act of 1999”.

4 **SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-**
5 **ICY.**

6 Chapter 35 of title 44, United States Code, is amend-
7 ed by inserting at the end the following:

8 ~~“SUBCHAPTER II—INFORMATION SECURITY~~

9 ~~“§ 3531. Purposes~~

10 ~~“The purposes of this subchapter are to—~~

11 ~~“(1) provide a comprehensive framework for es-~~
12 ~~tablishing and ensuring the effectiveness of controls~~
13 ~~over information resources that support Federal op-~~
14 ~~erations and assets;~~

15 ~~“(2)(A) recognize the highly networked nature~~
16 ~~of the Federal computing environment including the~~
17 ~~need for Federal Government interoperability and, in~~
18 ~~the implementation of improved security manage-~~
19 ~~ment measures, assure that opportunities for inter-~~
20 ~~operability are not adversely affected; and~~

21 ~~“(B) provide effective governmentwide manage-~~
22 ~~ment and oversight of the related information secu-~~
23 ~~rity risks, including coordination of information se-~~
24 ~~curity efforts throughout the civilian, national secu-~~
25 ~~rity, and law enforcement communities;~~

1 “(3) provide for development and maintenance
2 of minimum controls required to protect Federal in-
3 formation and information systems; and

4 “(4) provide a mechanism for improved over-
5 sight of Federal agency information security pro-
6 grams.

7 **“§ 3532. Definitions**

8 “(a) Except as provided under subsection (b), the
9 definitions under section 3502 shall apply to this sub-
10 chapter.

11 “(b) As used in this subchapter the term ‘information
12 technology’ has the meaning given that term in section
13 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

14 **“§ 3533. Authority and functions of the Director**

15 “(a)(1) Consistent with subchapter I, the Director
16 shall establish governmentwide policies for the manage-
17 ment of programs that support the cost-effective security
18 of Federal information systems by promoting security as
19 an integral component of each agency’s business oper-
20 ations.

21 “(2) Policies under this subsection shall—

22 “(A) be founded on a continuing risk manage-
23 ment cycle that recognizes the need to—

24 “(i) identify, assess, and understand risk;

25 and

1 “(ii) determine security needs commensu-
2 rate with the level of risk;

3 “(B) implement controls that adequately ad-
4 dress the risk;

5 “(C) promote continuing awareness of informa-
6 tion security risk;

7 “(D) continually monitor and evaluate policy;
8 and

9 “(E) control effectiveness of information secu-
10 rity practices.

11 “(b) The authority under subsection (a) includes the
12 authority to—

13 “(1) oversee and develop policies, principles,
14 standards, and guidelines for the handling of Fed-
15 eral information and information resources to im-
16 prove the efficiency and effectiveness of govern-
17 mental operations, including principles, policies, and
18 guidelines for the implementation of agency respon-
19 sibilities under applicable law for ensuring the pri-
20 vacy, confidentiality, and security of Federal infor-
21 mation;

22 “(2) consistent with the standards and guide-
23 lines promulgated under section 5131 of the Clinger-
24 Cohen Act of 1996 (40 U.S.C. 1441) and sections
25 5 and 6 of the Computer Security Act of 1987 (40

1 U.S.C. 759 note; Public Law 100-235, 101 Stat.
2 1729), require Federal agencies to identify and af-
3 ford security protections commensurate with the risk
4 and magnitude of the harm resulting from the loss,
5 misuse, or unauthorized access to or modification of
6 information collected or maintained by or on behalf
7 of an agency;

8 “(3) direct the heads of agencies to coordinate
9 such agencies and coordinate with industry to—

10 “(A) identify, use, and share best security
11 practices; and

12 “(B) develop voluntary consensus-based
13 standards for security controls, in a manner
14 consistent with section 2(b)(13) of the National
15 Institute of Standards and Technology Act (15
16 U.S.C. 272(b)(13));

17 “(4) oversee the development and implementa-
18 tion of standards and guidelines relating to security
19 controls for Federal computer systems by the Sec-
20 retary of Commerce through the National Institute
21 of Standards and Technology under section 5131 of
22 the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)
23 and section 20 of the National Institute of Stand-
24 ards and Technology Act (15 U.S.C. 278g-3);

1 “(5) oversee and coordinate compliance with
2 this section in a manner consistent with—

3 “(A) sections ~~552~~ and ~~552a~~ of title ~~5~~;

4 “(B) sections 20 and 21 of the National
5 Institute of Standards and Technology Act (~~15~~
6 U.S.C. ~~278g-3~~ and ~~278g-4~~);

7 “(C) section ~~5131~~ of the Clinger-Cohen
8 Act of 1996 (~~40~~ U.S.C. 1441);

9 “(D) sections ~~5~~ and ~~6~~ of the Computer Se-
10 curity Act of 1987 (~~40~~ U.S.C. ~~759~~ note; Public
11 Law ~~100-235~~; ~~101~~ Stat. 1729); and

12 “(E) related information management
13 laws; and

14 “(6) take any authorized action that the Direc-
15 tor considers appropriate, including any action in-
16 volving the budgetary process or appropriations
17 management process, to enforce accountability of the
18 head of an agency for information resources man-
19 agement and for the investments made by the agen-
20 cy in information technology, including—

21 “(A) recommending a reduction or an in-
22 crease in any amount for information resources
23 that the head of the agency proposes for the
24 budget submitted to Congress under section
25 ~~1105(a)~~ of title ~~31~~;

1 “(B) reducing or otherwise adjusting ap-
 2 portionments and reapportionments of appro-
 3 priations for information resources; and

4 “(C) using other authorized administrative
 5 controls over appropriations to restrict the
 6 availability of funds for information resources.

7 “(e) The authority under this section may be dele-
 8 gated only to the Deputy Director for Management of the
 9 Office of Management and Budget.

10 **“§ 3534. Federal agency responsibilities**

11 “(a) The head of each agency shall—

12 “(1) be responsible for—

13 “(A) adequately protecting the integrity,
 14 confidentiality, and availability of information
 15 and information systems supporting agency op-
 16 erations and assets; and

17 “(B) developing and implementing infor-
 18 mation security policies, procedures, and control
 19 techniques sufficient to afford security protec-
 20 tions commensurate with the risk and mag-
 21 nitude of the harm resulting from unauthorized
 22 disclosure, disruption, modification, or destruc-
 23 tion of information collected or maintained by
 24 or for the agency;

1 “(2) ensure that each senior program manager
2 is responsible for—

3 “(A) assessing the information security
4 risk associated with the operations and assets
5 of such manager;

6 “(B) determining the levels of information
7 security appropriate to protect the operations
8 and assets of such manager; and

9 “(C) periodically testing and evaluating in-
10 formation security controls and techniques;

11 “(3) delegate to the agency Chief Information
12 Officer established under section 3506, or a com-
13 parable official in an agency not covered by such
14 section, the authority to administer all functions
15 under this subchapter including—

16 “(A) designating a senior agency informa-
17 tion security officer;

18 “(B) developing and maintaining an agen-
19 cywide information security program as re-
20 quired under subsection (b);

21 “(C) ensuring that the agency effectively
22 implements and maintains information security
23 policies, procedures, and control techniques;

24 “(D) training and overseeing personnel
25 with significant responsibilities for information

1 security with respect to such responsibilities;
2 and

3 “(E) assisting senior program managers
4 concerning responsibilities under paragraph (2);

5 “(4) ensure that the agency has trained per-
6 sonnel sufficient to assist the agency in complying
7 with the requirements of this subchapter and related
8 policies, procedures, standards, and guidelines; and

9 “(5) ensure that the agency Chief Information
10 Officer, in coordination with senior program man-
11 agers, periodically—

12 “(A)(i) evaluates the effectiveness of the
13 agency information security program, including
14 testing control techniques; and

15 “(ii) implements appropriate remedial ac-
16 tions based on that evaluation; and

17 “(B) reports to the agency head on—

18 “(i) the results of such tests and eval-
19 uations; and

20 “(ii) the progress of remedial actions.

21 “(b)(1) Each agency shall develop and implement an
22 agencywide information security program to provide infor-
23 mation security for the operations and assets of the agen-
24 cy, including information security provided or managed by
25 another agency.

1 “(2) Each program under this subsection shall
2 include—

3 “(A) periodic assessments of information secu-
4 rity risks that consider internal and external threats
5 to—

6 “(i) the integrity, confidentiality, and
7 availability of systems; and

8 “(ii) data supporting critical operations
9 and assets;

10 “(B) policies and procedures that—

11 “(i) are based on the risk assessments re-
12 quired under paragraph (1) that cost-effectively
13 reduce information security risks to an accept-
14 able level; and

15 “(ii) ensure compliance with—

16 “(I) the requirements of this sub-
17 chapter;

18 “(II) policies and procedures as may
19 be prescribed by the Director; and

20 “(III) any other applicable require-
21 ments;

22 “(C) security awareness training to inform per-
23 sonnel of—

24 “(i) information security risks associated
25 with personnel activities; and

1 “(ii) responsibilities of personnel in com-
2 plying with agency policies and procedures de-
3 signed to reduce such risks;

4 “(D)(i) periodic management testing and eval-
5 uation of the effectiveness of information security
6 policies and procedures; and

7 “(ii) a process for ensuring remedial action to
8 address any deficiencies; and

9 “(E) procedures for detecting, reporting, and
10 responding to security incidents, including—

11 “(i) mitigating risks associated with such
12 incidents before substantial damage occurs;

13 “(ii) notifying and consulting with law en-
14 forcement officials and other offices and au-
15 thorities; and

16 “(iii) notifying and consulting with an of-
17 fice designated by the Administrator of General
18 Services within the General Services Adminis-
19 tration.

20 “(3) Each program under this subsection is subject
21 to the approval of the Director and is required to be re-
22 viewed at least annually by agency program officials in
23 consultation with the Chief Information Officer.

1 “(c)(1) Each agency shall examine the adequacy and
 2 effectiveness of information security policies, procedures,
 3 and practices in plans and reports relating to—

4 “(A) annual agency budgets;

5 “(B) information resources management under
 6 the Paperwork Reduction Act of 1995 (44 U.S.C.
 7 401 note);

8 “(C) program performance under sections 1105
 9 and 1115 through 1119 of title 31, and sections
 10 2801 through 2805 of title 39; and

11 “(D) financial management under—

12 “(i) chapter 9 of title 31, United States
 13 Code, and the Chief Financial Officers Act of
 14 1990 (31 U.S.C. 501 note; Public Law 101–
 15 576) (and the amendments made by that Act);

16 “(ii) the Federal Financial Management
 17 Improvement Act of 1996 (31 U.S.C. 3512
 18 note) (and the amendments made by that Act);
 19 and

20 “(iii) the internal controls conducted under
 21 section 3512 of title 31.

22 “(2) Any deficiency in a policy, procedure, or practice
 23 identified under paragraph (1) shall be reported as a ma-
 24 terial weakness in reporting required under the applicable
 25 provision of law under paragraph (1).

1 **~~“§ 3535. Annual independent evaluation~~**

2 ~~“(a)(1) Each year each agency shall have an inde-~~
 3 ~~pendent evaluation performed of the information security~~
 4 ~~program and practices of that agency.~~

5 ~~“(2) Each evaluation under this section shall~~
 6 ~~include—~~

7 ~~“(A) an assessment of compliance with—~~

8 ~~“(i) the requirements of this subchapter;~~
 9 ~~and~~

10 ~~“(ii) related information security policies;~~
 11 ~~procedures, standards, and guidelines; and~~

12 ~~“(B) tests of the effectiveness of information~~
 13 ~~security control techniques.~~

14 ~~“(b)(1) For agencies with Inspectors General ap-~~
 15 ~~pointed under the Inspector General Act of 1978 (5~~
 16 ~~U.S.C. App.); annual evaluations required under this sec-~~
 17 ~~tion shall be performed by the Inspector General or by~~
 18 ~~an independent external auditor, as determined by the In-~~
 19 ~~spector General of the agency.~~

20 ~~“(2) For any agency to which paragraph (1) does not~~
 21 ~~apply, the head of the agency shall contract with an inde-~~
 22 ~~pendent external auditor to perform the evaluation.~~

23 ~~“(3) An evaluation of agency information security~~
 24 ~~programs and practices performed by the Comptroller~~
 25 ~~General may be in lieu of the evaluation required under~~
 26 ~~this section.~~

1 “(c) Not later than March 1, 2001, and every March
2 1 thereafter, the results of an evaluation required under
3 this section shall be submitted to the Director.

4 “(d) Each year the Comptroller General shall—

5 “(1) review the evaluations required under this
6 section and other information security evaluation re-
7 sults; and

8 “(2) report to Congress regarding the adequacy
9 of agency information programs and practices.

10 “(e) Agencies and auditors shall take appropriate ac-
11 tions to ensure the protection of information, the disclo-
12 sure of which may adversely affect information security.
13 Such protections shall be commensurate with the risk and
14 comply with all applicable laws.”.

15 **SEC. 3. RESPONSIBILITIES OF CERTAIN AGENCIES.**

16 (a) DEPARTMENT OF COMMERCE.—The Secretary of
17 Commerce, through the National Institute of Standards
18 and Technology and with technical assistance from the
19 National Security Agency, shall—

20 (1) develop, issue, review, and update standards
21 and guidance for the security of information in Fed-
22 eral computer systems, including development of
23 methods and techniques for security systems and
24 validation programs;

1 (2) develop, issue, review, and update guidelines
2 for training in computer security awareness and ac-
3 cepted computer security practices, with assistance
4 from the Office of Personnel Management;

5 (3) provide agencies with guidance for security
6 planning to assist in the development of applications
7 and system security plans for such agencies;

8 (4) provide guidance and assistance to agencies
9 concerning cost-effective controls when inter-
10 connecting with other systems; and

11 (5) evaluate information technologies to assess
12 security vulnerabilities and alert Federal agencies of
13 such vulnerabilities.

14 (b) DEPARTMENT OF JUSTICE.—The Department of
15 Justice shall review and update guidance to agencies on—

16 (1) legal remedies regarding security incidents
17 and ways to report to and work with law enforce-
18 ment agencies concerning such incidents; and

19 (2) permitted uses of security techniques and
20 technologies.

21 (c) GENERAL SERVICES ADMINISTRATION.—The
22 General Services Administration shall—

23 (1) review and update General Services Admin-
24 istration guidance to agencies on addressing security

1 considerations when acquiring information tech-
 2 nology; and

3 ~~(2) assist agencies in the acquisition of cost-ef-~~
 4 ~~fective security products, services, and incident re-~~
 5 ~~sponse capabilities.~~

6 ~~(d) OFFICE OF PERSONNEL MANAGEMENT.—The~~
 7 ~~Office of Personnel Management shall—~~

8 ~~(1) review and update Office of Personnel Man-~~
 9 ~~agement regulations concerning computer security~~
 10 ~~training for Federal civilian employees; and~~

11 ~~(2) assist the Department of Commerce in up-~~
 12 ~~dating and maintaining guidelines for training in~~
 13 ~~computer security awareness and computer security~~
 14 ~~best practices.~~

15 **SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.**

16 ~~(a) IN GENERAL.—Chapter 35 of title 44, United~~
 17 ~~States Code, is amended—~~

18 ~~(1) in the table of sections—~~

19 ~~(A) by inserting after the chapter heading~~
 20 ~~the following:~~

~~“SUBCHAPTER I—FEDERAL INFORMATION POLICY”;~~

21 ~~and~~

22 ~~(B) by inserting after the item relating to~~
 23 ~~section 3520 the following:~~

~~“SUBCHAPTER II—INFORMATION SECURITY~~

~~“Sec.~~

~~“3531. Purposes.~~

(2) by inserting before section 3501 the following:

6 (b) REFERENCES TO CHAPTER 35.—Chapter 35 of
7 title 44, United States Code, is amended—

(A) in the matter preceding paragraph (1);
by striking “chapter” and inserting “sub-
chapter”; and

(2) in section 3502, in the matter preceding paragraph (1), by striking “chapter” and inserting “subchapter”;

19 ~~(4) in section 3504—~~

22 (B) in subsection (d)(2), by striking
23 “chapter” and inserting “subchapter”; and

1 (C) in subsection (f)(1), by striking “chap-
2 ter” and inserting “subchapter”;

3 (5) in section 3505—

4 (A) in subsection (a), in the matter pre-
5 ceding paragraph (1), by striking “chapter”
6 and inserting “subchapter”;

7 (B) in subsection (a)(2), by striking “chap-
8 ter” and inserting “subchapter”; and

9 (C) in subsection (a)(3)(B)(iii), by striking
10 “chapter” and inserting “subchapter”;

11 (6) in section 3506—

12 (A) in subsection (a)(1)(B), by striking
13 “chapter” and inserting “subchapter”;

14 (B) in subsection (a)(2)(A), by striking
15 “chapter” and inserting “subchapter”;

16 (C) in subsection (a)(2)(B), by striking
17 “chapter” and inserting “subchapter”;

18 (D) in subsection (a)(3)—

19 (i) in the first sentence, by striking
20 “chapter” and inserting “subchapter”; and

21 (ii) in the second sentence, by striking
22 “chapter” and inserting “subchapter”;

23 (E) in subsection (b)(4), by striking “chap-
24 ter” and inserting “subchapter”;

1 ~~(F)~~ in subsection ~~(c)~~(1), by striking “chap-
2 ter, to” and inserting “subchapter, to”; and

3 ~~(G)~~ in subsection ~~(c)~~(1)(A), by striking
4 “chapter” and inserting “subchapter”;
5 ~~(7)~~ in section 3507—

6 ~~(A)~~ in subsection ~~(c)~~(3)(B), by striking
7 “chapter” and inserting “subchapter”;

8 ~~(B)~~ in subsection ~~(h)~~(2)(B), by striking
9 “chapter” and inserting “subchapter”;

10 ~~(C)~~ in subsection ~~(h)~~(3), by striking “chap-
11 ter” and inserting “subchapter”;

12 ~~(D)~~ in subsection ~~(j)~~(1)(A)(i), by striking
13 “chapter” and inserting “subchapter”;

14 ~~(E)~~ in subsection ~~(j)~~(1)(B), by striking
15 “chapter” and inserting “subchapter”; and

16 ~~(F)~~ in subsection ~~(j)~~(2), by striking “chap-
17 ter” and inserting “subchapter”;

18 ~~(8)~~ in section 3509, by striking “chapter” and
19 inserting “subchapter”;

20 ~~(9)~~ in section 3512—

21 ~~(A)~~ in subsection ~~(a)~~, by striking “chapter
22 if” and inserting “subchapter if”; and

23 ~~(B)~~ in subsection ~~(a)~~(1), by striking “chap-
24 ter” and inserting “subchapter”;

25 ~~(10)~~ in section 3514—

1 (A) in subsection (a)(1)(A), by striking
2 “chapter” and inserting “subchapter”; and

3 (B) in subsection (a)(2)(A)(ii), by striking
4 “chapter” and inserting “subchapter” each
5 place it appears;

6 (11) in section 3515, by striking “chapter” and
7 inserting “subchapter”;

8 (12) in section 3516, by striking “chapter” and
9 inserting “subchapter”;

10 (13) in section 3517(b), by striking “chapter”
11 and inserting “subchapter”;

12 (14) in section 3518—

13 (A) in subsection (a), by striking “chap-
14 ter” and inserting “subchapter” each place it
15 appears;

16 (B) in subsection (b), by striking “chap-
17 ter” and inserting “subchapter”;

18 (C) in subsection (c)(1), by striking “chap-
19 ter” and inserting “subchapter”;

20 (D) in subsection (c)(2), by striking “chap-
21 ter” and inserting “subchapter”;

22 (E) in subsection (d), by striking “chap-
23 ter” and inserting “subchapter”; and

24 (F) in subsection (e), by striking “chap-
25 ter” and inserting “subchapter”; and

1 (15) in section 3520, by striking “chapter” and
 2 inserting “subchapter”.

3 **SEC. 5. EFFECTIVE DATE.**

4 This Act and the amendments made by this Act shall
 5 take effect 30 days after the date of enactment of this
 6 Act.

7 **SECTION 1. SHORT TITLE.**

8 *This Act may be cited as the “Government Information*
 9 *Security Act”.*

10 **SEC. 2. COORDINATION OF FEDERAL INFORMATION**
 11 **POLICY.**

12 *Chapter 35 of title 44, United States Code, is amended*
 13 *by inserting at the end the following:*

14 **“SUBCHAPTER II—INFORMATION SECURITY**

15 **“§ 3531. Purposes**

16 *“The purposes of this subchapter are to—*

17 *“(1) provide a comprehensive framework for es-*
 18 *tablishing and ensuring the effectiveness of controls*
 19 *over information resources that support Federal oper-*
 20 *ations and assets;*

21 *“(2)(A) recognize the highly networked nature of*
 22 *the Federal computing environment including the*
 23 *need for Federal Government interoperability and, in*
 24 *the implementation of improved security management*

1 *measures, assure that opportunities for interoper-*
 2 *ability are not adversely affected; and*

3 *“(B) provide effective governmentwide manage-*
 4 *ment and oversight of the related information security*
 5 *risks, including coordination of information security*
 6 *efforts throughout the civilian, national security, and*
 7 *law enforcement communities;*

8 *“(3) provide for development and maintenance of*
 9 *minimum controls required to protect Federal infor-*
 10 *mation and information systems; and*

11 *“(4) provide a mechanism for improved oversight*
 12 *of Federal agency information security programs.*

13 **“§ 3532. Definitions**

14 *“(a) Except as provided under subsection (b), the defi-*
 15 *nitions under section 3502 shall apply to this subchapter.*

16 *“(b) As used in this subchapter the term—*

17 *“(1) ‘information technology’ has the meaning*
 18 *given that term in section 5002 of the Clinger-Cohen*
 19 *Act of 1996 (40 U.S.C. 1401); and*

20 *“(2) ‘mission critical system’ means any tele-*
 21 *communications or information system used or oper-*
 22 *ated by an agency or by a contractor of an agency,*
 23 *or other organization on behalf of an agency, that—*

1 “(A) is defined as a national security sys-
 2 tem under section 5142 of the Clinger-Cohen Act
 3 of 1996 (40 U.S.C. 1452);

4 “(B) is protected at all times by procedures
 5 established for information which has been spe-
 6 cifically authorized under criteria established by
 7 an Executive order or an Act of Congress to be
 8 kept secret in the interest of national defense or
 9 foreign policy; or

10 “(C) processes any information, the loss,
 11 misuse, disclosure, or unauthorized access to or
 12 modification of, would have a debilitating im-
 13 pact on the mission of an agency.

14 **“§ 3533. Authority and functions of the Director**

15 “(a)(1) The Director shall establish governmentwide
 16 policies for the management of programs that—

17 “(A) support the cost-effective security of Federal
 18 information systems by promoting security as an in-
 19 tegral component of each agency’s business operations;
 20 and

21 “(B) include information technology architec-
 22 tures as defined under section 5125 of the Clinger-
 23 Cohen Act of 1996 (40 U.S.C. 1425).

24 “(2) Policies under this subsection shall—

1 “(A) be founded on a continuing risk manage-
2 ment cycle that recognizes the need to—

3 “(i) identify, assess, and understand risk;
4 and

5 “(ii) determine security needs commensu-
6 rate with the level of risk;

7 “(B) implement controls that adequately address
8 the risk;

9 “(C) promote continuing awareness of informa-
10 tion security risk; and

11 “(D) continually monitor and evaluate policy
12 and control effectiveness of information security prac-
13 tices.

14 “(b) The authority under subsection (a) includes the
15 authority to—

16 “(1) oversee and develop policies, principles,
17 standards, and guidelines for the handling of Federal
18 information and information resources to improve the
19 efficiency and effectiveness of governmental oper-
20 ations, including principles, policies, and guidelines
21 for the implementation of agency responsibilities
22 under applicable law for ensuring the privacy, con-
23 fidentiality, and security of Federal information;

24 “(2) consistent with the standards and guidelines
25 promulgated under section 5131 of the Clinger-Cohen

1 *Act of 1996 (40 U.S.C. 1441) and sections 5 and 6*
2 *of the Computer Security Act of 1987 (40 U.S.C.*
3 *1441 note; Public Law 100–235; 101 Stat. 1729), re-*
4 *quire Federal agencies to identify and afford security*
5 *protections commensurate with the risk and mag-*
6 *nitude of the harm resulting from the loss, misuse,*
7 *or unauthorized access to or modification of informa-*
8 *tion collected or maintained by or on behalf of an*
9 *agency;*

10 *“(3) direct the heads of agencies to—*

11 *“(A) identify, use, and share best security*
12 *practices;*

13 *“(B) develop an agency-wide information*
14 *security plan;*

15 *“(C) incorporate information security prin-*
16 *ciples and practices throughout the life cycles of*
17 *the agency’s information systems; and*

18 *“(D) ensure that the agency’s information*
19 *security plan is practiced throughout all life cy-*
20 *cles of the agency’s information systems;*

21 *“(4) oversee the development and implementation*
22 *of standards and guidelines relating to security con-*
23 *trols for Federal computer systems by the Secretary of*
24 *Commerce through the National Institute of Stand-*
25 *ards and Technology under section 5131 of the*

1 *Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sec-*
 2 *tion 20 of the National Institute of Standards and*
 3 *Technology Act (15 U.S.C. 278g-3);*

4 *“(5) oversee and coordinate compliance with this*
 5 *section in a manner consistent with—*

6 *“(A) sections 552 and 552a of title 5;*

7 *“(B) sections 20 and 21 of the National In-*
 8 *stitute of Standards and Technology Act (15*
 9 *U.S.C. 278g-3 and 278g-4);*

10 *“(C) section 5131 of the Clinger-Cohen Act*
 11 *of 1996 (40 U.S.C. 1441);*

12 *“(D) sections 5 and 6 of the Computer Se-*
 13 *curity Act of 1987 (40 U.S.C. 1441 note; Public*
 14 *Law 100-235; 101 Stat. 1729); and*

15 *“(E) related information management laws;*
 16 *and*

17 *“(6) take any authorized action under section*
 18 *5113(b)(5) of the Clinger-Cohen Act of 1996 (40*
 19 *U.S.C. 1413(b)(5)) that the Director considers appro-*
 20 *priate, including any action involving the budgetary*
 21 *process or appropriations management process, to en-*
 22 *force accountability of the head of an agency for in-*
 23 *formation resources management, including the re-*
 24 *quirements of this subchapter, and for the investments*

1 *made by the agency in information technology,*
 2 *including—*

3 “(A) *recommending a reduction or an in-*
 4 *crease in any amount for information resources*
 5 *that the head of the agency proposes for the*
 6 *budget submitted to Congress under section*
 7 *1105(a) of title 31;*

8 “(B) *reducing or otherwise adjusting appor-*
 9 *tionments and reapportionments of appropria-*
 10 *tions for information resources; and*

11 “(C) *using other authorized administrative*
 12 *controls over appropriations to restrict the avail-*
 13 *ability of funds for information resources.*

14 “(c) *The authorities of the Director under this section*
 15 *may be delegated—*

16 “(1) *to the Secretary of Defense and the Director*
 17 *of Central Intelligence in the case of systems described*
 18 *under subparagraphs (A) and (B) of section*
 19 *3532(b)(2); and*

20 “(2) *in the case of all other Federal information*
 21 *systems, only to the Deputy Director for Management*
 22 *of the Office of Management and Budget.*

23 **“§ 3534. Federal agency responsibilities**

24 “(a) *The head of each agency shall—*

25 “(1) *be responsible for—*

1 “(A) adequately ensuring the integrity, con-
2 fidentiality, authenticity, availability, and non-
3 repudiation of information and information sys-
4 tems supporting agency operations and assets;

5 “(B) developing and implementing informa-
6 tion security policies, procedures, and control
7 techniques sufficient to afford security protec-
8 tions commensurate with the risk and magnitude
9 of the harm resulting from unauthorized disclo-
10 sure, disruption, modification, or destruction of
11 information collected or maintained by or for the
12 agency; and

13 “(C) ensuring that the agency’s information
14 security plan is practiced throughout the life
15 cycle of each agency system;

16 “(2) ensure that appropriate senior agency offi-
17 cials are responsible for—

18 “(A) assessing the information security
19 risks associated with the operations and assets
20 for programs and systems over which such offi-
21 cials have control;

22 “(B) determining the levels of information
23 security appropriate to protect such operations
24 and assets; and

1 “(C) periodically testing and evaluating in-
2 formation security controls and techniques;

3 “(3) delegate to the agency Chief Information Of-
4 ficer established under section 3506, or a comparable
5 official in an agency not covered by such section, the
6 authority to administer all functions under this sub-
7 chapter including—

8 “(A) designating a senior agency informa-
9 tion security official who shall report to the
10 Chief Information Officer or a comparable offi-
11 cial;

12 “(B) developing and maintaining an agen-
13 cywide information security program as required
14 under subsection (b);

15 “(C) ensuring that the agency effectively
16 implements and maintains information security
17 policies, procedures, and control techniques;

18 “(D) training and overseeing personnel
19 with significant responsibilities for information
20 security with respect to such responsibilities; and

21 “(E) assisting senior agency officials con-
22 cerning responsibilities under paragraph (2);

23 “(4) ensure that the agency has trained per-
24 sonnel sufficient to assist the agency in complying

1 *with the requirements of this subchapter and related*
 2 *policies, procedures, standards, and guidelines; and*

3 “(5) *ensure that the agency Chief Information*
 4 *Officer, in coordination with senior agency officials,*
 5 *periodically—*

6 “(A)(i) *evaluates the effectiveness of the*
 7 *agency information security program, including*
 8 *testing control techniques; and*

9 “(ii) *implements appropriate remedial ac-*
 10 *tions based on that evaluation; and*

11 “(B) *reports to the agency head on—*

12 “(i) *the results of such tests and eval-*
 13 *uations; and*

14 “(ii) *the progress of remedial actions.*

15 “(b)(1) *Each agency shall develop and implement an*
 16 *agencywide information security program to provide infor-*
 17 *mation security for the operations and assets of the agency,*
 18 *including operations and assets provided or managed by*
 19 *another agency.*

20 “(2) *Each program under this subsection shall*
 21 *include—*

22 “(A) *periodic risk assessments that consider in-*
 23 *ternal and external threats to—*

24 “(i) *the integrity, confidentiality, and*
 25 *availability of systems; and*

1 “(ii) data supporting critical operations
2 and assets;

3 “(B) policies and procedures that—

4 “(i) are based on the risk assessments re-
5 quired under subparagraph (A) that cost-effec-
6 tively reduce information security risks to an ac-
7 ceptable level; and

8 “(ii) ensure compliance with—

9 “(I) the requirements of this sub-
10 chapter;

11 “(II) policies and procedures as may
12 be prescribed by the Director; and

13 “(III) any other applicable require-
14 ments;

15 “(C) security awareness training to inform per-
16 sonnel of—

17 “(i) information security risks associated
18 with the activities of personnel; and

19 “(ii) responsibilities of personnel in com-
20 plying with agency policies and procedures de-
21 signed to reduce such risks;

22 “(D)(i) periodic management testing and evalua-
23 tion of the effectiveness of information security poli-
24 cies and procedures; and

1 “(ii) a process for ensuring remedial action to
2 address any significant deficiencies; and

3 “(E) procedures for detecting, reporting, and re-
4 sponding to security incidents, including—

5 “(i) mitigating risks associated with such
6 incidents before substantial damage occurs;

7 “(ii) notifying and consulting with law en-
8 forcement officials and other offices and authori-
9 ties;

10 “(iii) notifying and consulting with an of-
11 fice designated by the Administrator of General
12 Services within the General Services Administra-
13 tion; and

14 “(iv) notifying and consulting with an of-
15 fice designated by the Secretary of Defense and
16 the Director of Central Intelligence for incidents
17 involving systems described under subparagraphs
18 (A) and (B) of section 3532(b)(2).

19 “(3) Each program under this subsection is subject to
20 the approval of the Director and is required to be reviewed
21 at least annually by agency program officials in consulta-
22 tion with the Chief Information Officer. In the case of sys-
23 tems described under subparagraphs (A) and (B) of section
24 3532(b)(2), the Director shall delegate approval authority

1 *under this paragraph to the Secretary of Defense and the*
 2 *Director of Central Intelligence.*

3 “(c)(1) *Each agency shall examine the adequacy and*
 4 *effectiveness of information security policies, procedures,*
 5 *and practices in plans and reports relating to—*

6 “(A) *annual agency budgets;*

7 “(B) *information resources management under*
 8 *the Paperwork Reduction Act of 1995 (44 U.S.C. 101*
 9 *note);*

10 “(C) *performance and results based management*
 11 *under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401*
 12 *et seq.);*

13 “(D) *program performance under sections 1105*
 14 *and 1115 through 1119 of title 31, and sections 2801*
 15 *through 2805 of title 39; and*

16 “(E) *financial management under—*

17 “(i) *chapter 9 of title 31, United States*
 18 *Code, and the Chief Financial Officers Act of*
 19 *1990 (31 U.S.C. 501 note; Public Law 101–576)*
 20 *(and the amendments made by that Act);*

21 “(ii) *the Federal Financial Management*
 22 *Improvement Act of 1996 (31 U.S.C. 3512 note)*
 23 *(and the amendments made by that Act); and*

24 “(iii) *the internal controls conducted under*
 25 *section 3512 of title 31.*

1 “(2) *Any significant deficiency in a policy, procedure,*
 2 *or practice identified under paragraph (1) shall be reported*
 3 *as a material weakness in reporting required under the ap-*
 4 *plicable provision of law under paragraph (1).*

5 “(d)(1) *In addition to the requirements of subsection*
 6 *(c), each agency, in consultation with the Chief Information*
 7 *Officer, shall include as part of the performance plan re-*
 8 *quired under section 1115 of title 31 a description of—*

9 “(A) *the time periods; and*

10 “(B) *the resources, including budget, staffing,*
 11 *and training,*

12 *which are necessary to implement the program required*
 13 *under subsection (b)(1).*

14 “(2) *The description under paragraph (1) shall be*
 15 *based on the risk assessment required under subsection*
 16 *(b)(2)(A).*

17 **“§ 3535. Annual independent evaluation**

18 “(a)(1) *Each year each agency shall have performed*
 19 *an independent evaluation of the information security pro-*
 20 *gram and practices of that agency.*

21 “(2) *Each evaluation under this section shall*
 22 *include—*

23 “(A) *an assessment of compliance with—*

24 “(i) *the requirements of this subchapter;*

25 *and*

1 “(ii) related information security policies,
2 procedures, standards, and guidelines; and

3 “(B) tests of the effectiveness of information secu-
4 rity control techniques.

5 “(3) The Inspector General or the independent eval-
6 uator performing an evaluation under this section includ-
7 ing the Comptroller General may use any audit, evaluation,
8 or report relating to programs or practices of the applicable
9 agency.

10 “(b)(1)(A) Subject to subparagraph (B), for agencies
11 with Inspectors General appointed under the Inspector Gen-
12 eral Act of 1978 (5 U.S.C. App.) or any other law, the an-
13 nual evaluation required under this section or, in the case
14 of systems described under subparagraphs (A) and (B) of
15 section 3532(b)(2), an audit of the annual evaluation re-
16 quired under this section, shall be performed by the Inspec-
17 tor General or by an independent evaluator, as determined
18 by the Inspector General of the agency.

19 “(B) For systems described under subparagraphs (A)
20 and (B) of section 3532(b)(2), the evaluation required under
21 this section shall be performed only by an entity designated
22 by the Secretary of Defense or the Director of Central Intel-
23 ligence as appropriate.

1 “(2) *For any agency to which paragraph (1) does not*
 2 *apply, the head of the agency shall contract with an inde-*
 3 *pendent evaluator to perform the evaluation.*

4 “(3) *An evaluation of agency information security*
 5 *programs and practices performed by the Comptroller Gen-*
 6 *eral may be in lieu of the evaluation required under this*
 7 *section.*

8 “(c) *Not later than 1 year after the date of enactment*
 9 *of this subchapter, and on that date every year thereafter,*
 10 *the applicable agency head shall submit to the Director—*

11 “(1) *the results of each evaluation required under*
 12 *this section, other than an evaluation of a system de-*
 13 *scribed under subparagraph (A) or (B) of section*
 14 *3532(b)(2); and*

15 “(2) *the results of each audit of an evaluation re-*
 16 *quired under this section of a system described under*
 17 *subparagraph (A) or (B) of section 3532(b)(2).*

18 “(d) *Each year the Comptroller General shall—*

19 “(1) *review the evaluations required under this*
 20 *section and other information security evaluation re-*
 21 *sults; and*

22 “(2) *report to Congress regarding the adequacy*
 23 *of agency information programs and practices.*

24 “(e) *Agencies and evaluators shall take appropriate ac-*
 25 *tions to ensure the protection of information, the disclosure*

1 *of which may adversely affect information security. Such*
 2 *protections shall be commensurate with the risk and comply*
 3 *with all applicable laws.”.*

4 **SEC. 3. RESPONSIBILITIES OF CERTAIN AGENCIES.**

5 (a) *DEPARTMENT OF COMMERCE.—Notwithstanding*
 6 *section 20 of the National Institute of Standards and Tech-*
 7 *nology Act (15 U.S.C. 278g–3) and except as provided*
 8 *under subsection (b), the Secretary of Commerce, through*
 9 *the National Institute of Standards and Technology and*
 10 *with technical assistance from the National Security Agen-*
 11 *cy, as required or when requested, shall—*

12 (1) *develop, issue, review, and update standards*
 13 *and guidance for the security of Federal information*
 14 *systems, including development of methods and tech-*
 15 *niques for security systems and validation programs;*

16 (2) *develop, issue, review, and update guidelines*
 17 *for training in computer security awareness and ac-*
 18 *cepted computer security practices, with assistance*
 19 *from the Office of Personnel Management;*

20 (3) *provide agencies with guidance for security*
 21 *planning to assist in the development of applications*
 22 *and system security plans for such agencies;*

23 (4) *provide guidance and assistance to agencies*
 24 *concerning cost-effective controls when interconnecting*
 25 *with other systems; and*

1 (5) *evaluate information technologies to assess se-*
 2 *curity vulnerabilities and alert Federal agencies of*
 3 *such vulnerabilities as soon as those vulnerabilities*
 4 *are known.*

5 (b) *DEPARTMENT OF DEFENSE AND THE INTEL-*
 6 *LIGENCE COMMUNITY.*—*Notwithstanding section 3533 of*
 7 *title 44, United States Code (as added by section 2 of this*
 8 *Act), the Secretary of Defense and the Director of Central*
 9 *Intelligence, shall, consistent with their respective*
 10 *authorities—*

11 (1) *develop and issue information security poli-*
 12 *cies, standards, and guidelines for systems described*
 13 *under subparagraphs (A) and (B) of section*
 14 *3532(b)(2) of title 44, United States Code (as added*
 15 *by section 2 of this Act), that provide more stringent*
 16 *protection than the policies, principles, standards,*
 17 *and guidelines required under section 3533 of such*
 18 *title; and*

19 (2) *ensure the implementation of the information*
 20 *security policies, principles, standards, and guidelines*
 21 *described under paragraph (1).*

22 (c) *DEPARTMENT OF JUSTICE.*—*The Department of*
 23 *Justice shall review and update guidance to agencies on—*

1 (1) *legal remedies regarding security incidents*
 2 *and ways to report to and work with law enforcement*
 3 *agencies concerning such incidents; and*

4 (2) *lawful uses of security techniques and tech-*
 5 *nologies.*

6 (d) *GENERAL SERVICES ADMINISTRATION.—The Gen-*
 7 *eral Services Administration shall—*

8 (1) *review and update General Services Admin-*
 9 *istration guidance to agencies on addressing security*
 10 *considerations when acquiring information tech-*
 11 *nology; and*

12 (2) *assist agencies in—*

13 (A) *fulfilling agency responsibilities under*
 14 *section 3534(b)(2)(E) of title 44, United States*
 15 *Code (as added by section 2 of this Act); and*

16 (B) *the acquisition of cost-effective security*
 17 *products, services, and incident response capa-*
 18 *bilities.*

19 (e) *OFFICE OF PERSONNEL MANAGEMENT.—The Office*
 20 *of Personnel Management shall—*

21 (1) *review and update Office of Personnel Man-*
 22 *agement regulations concerning computer security*
 23 *training for Federal civilian employees;*

24 (2) *assist the Department of Commerce in updat-*
 25 *ing and maintaining guidelines for training in com-*

1 puter security awareness and computer security best
2 practices; and

3 (3) *work with the National Science Foundation*
4 *and other agencies on personnel and training initia-*
5 *tives (including scholarships and fellowships, as au-*
6 *thorized by law) as necessary to ensure that the Fed-*
7 *eral Government—*

8 (A) *has adequate sources of continuing in-*
9 *formation security education and training avail-*
10 *able for employees; and*

11 (B) *has an adequate supply of qualified in-*
12 *formation security professionals to meet agency*
13 *needs.*

14 (f) *INFORMATION SECURITY POLICIES, PRINCIPLES,*
15 *STANDARDS, AND GUIDELINES.—Notwithstanding any pro-*
16 *vision of this Act (including any amendment made by this*
17 *Act)—*

18 (1) *the Secretary of Defense and the Director of*
19 *Central Intelligence shall develop such policies, prin-*
20 *ciples, procedures, and guidelines for mission critical*
21 *systems subject to their control;*

22 (2) *the policies, principles, procedures, and*
23 *guidelines developed by the Secretary of Defense and*
24 *the Director of Central Intelligence may be adopted,*
25 *to the extent that such policies are consistent with*

1 *policies and guidance developed by the Director of the*
 2 *Office of Management and Budget and the Secretary*
 3 *of Commerce—*

4 *(A) by the Director of the Office of Manage-*
 5 *ment and Budget, as appropriate, to the mission*
 6 *critical systems of all agencies; or*

7 *(B) by an agency head, as appropriate, to*
 8 *the mission critical systems of that agency; and*

9 *(3) to the extent that such policies are consistent*
 10 *with policies and guidance developed by the Director*
 11 *of the Office of Management and Budget and the Sec-*
 12 *retary of Commerce, an agency may develop and im-*
 13 *plement information security policies, principles,*
 14 *standards, and guidelines that provide more stringent*
 15 *protection than those required under section 3533 of*
 16 *title 44, United States Code (as added by section 2*
 17 *of this Act), or subsection (a) of this section.*

18 **SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.**

19 *(a) IN GENERAL.—Chapter 35 of title 44, United*
 20 *States Code, is amended—*

21 *(1) in the table of sections—*

22 *(A) by inserting after the chapter heading*
 23 *the following:*

“SUBCHAPTER I—FEDERAL INFORMATION POLICY”;

24 *and*

1 (B) by inserting after the item relating to
2 section 3520 the following:

“SUBCHAPTER II—INFORMATION SECURITY

“Sec.

“3531. Purposes.

“3532. Definitions.

“3533. Authority and functions of the Director.

“3534. Federal agency responsibilities.

“3535. Annual independent evaluation.”;

3 and

4 (2) by inserting before section 3501 the following:

5 “SUBCHAPTER I—FEDERAL INFORMATION
6 POLICY”.

7 (b) REFERENCES TO CHAPTER 35.—Chapter 35 of title
8 44, United States Code, is amended—

9 (1) in section 3501—

10 (A) in the matter preceding paragraph (1),
11 by striking “chapter” and inserting “sub-
12 chapter”; and

13 (B) in paragraph (11), by striking “chap-
14 ter” and inserting “subchapter”;

15 (2) in section 3502, in the matter preceding
16 paragraph (1), by striking “chapter” and inserting
17 “subchapter”;

18 (3) in section 3503, in subsection (b), by striking
19 “chapter” and inserting “subchapter”;

20 (4) in section 3504—

21 (A) in subsection (a)(2), by striking “chap-
22 ter” and inserting “subchapter”;

1 (B) in subsection (d)(2), by striking “chap-
2 ter” and inserting “subchapter”; and

3 (C) in subsection (f)(1), by striking “chap-
4 ter” and inserting “subchapter”;

5 (5) in section 3505—

6 (A) in subsection (a), in the matter pre-
7 ceding paragraph (1), by striking “chapter” and
8 inserting “subchapter”;

9 (B) in subsection (a)(2), by striking “chap-
10 ter” and inserting “subchapter”; and

11 (C) in subsection (a)(3)(B)(iii), by striking
12 “chapter” and inserting “subchapter”;

13 (6) in section 3506—

14 (A) in subsection (a)(1)(B), by striking
15 “chapter” and inserting “subchapter”;

16 (B) in subsection (a)(2)(A), by striking
17 “chapter” and inserting “subchapter”;

18 (C) in subsection (a)(2)(B), by striking
19 “chapter” and inserting “subchapter”;

20 (D) in subsection (a)(3)—

21 (i) in the first sentence, by striking
22 “chapter” and inserting “subchapter”; and

23 (ii) in the second sentence, by striking
24 “chapter” and inserting “subchapter”;

1 (E) in subsection (b)(4), by striking “chap-
2 ter” and inserting “subchapter”;

3 (F) in subsection (c)(1), by striking “chap-
4 ter, to” and inserting “subchapter, to”; and

5 (G) in subsection (c)(1)(A), by striking
6 “chapter” and inserting “subchapter”;

7 (7) in section 3507—

8 (A) in subsection (e)(3)(B), by striking
9 “chapter” and inserting “subchapter”;

10 (B) in subsection (h)(2)(B), by striking
11 “chapter” and inserting “subchapter”;

12 (C) in subsection (h)(3), by striking “chap-
13 ter” and inserting “subchapter”;

14 (D) in subsection (j)(1)(A)(i), by striking
15 “chapter” and inserting “subchapter”;

16 (E) in subsection (j)(1)(B), by striking
17 “chapter” and inserting “subchapter”; and

18 (F) in subsection (j)(2), by striking “chap-
19 ter” and inserting “subchapter”;

20 (8) in section 3509, by striking “chapter” and
21 inserting “subchapter”;

22 (9) in section 3512—

23 (A) in subsection (a), by striking “chapter
24 if” and inserting “subchapter if”; and

1 (B) in subsection (a)(1), by striking “chap-
2 ter” and inserting “subchapter”;

3 (10) in section 3514—

4 (A) in subsection (a)(1)(A), by striking
5 “chapter” and inserting “subchapter”; and

6 (B) in subsection (a)(2)(A)(ii), by striking
7 “chapter” and inserting “subchapter” each place
8 it appears;

9 (11) in section 3515, by striking “chapter” and
10 inserting “subchapter”;

11 (12) in section 3516, by striking “chapter” and
12 inserting “subchapter”;

13 (13) in section 3517(b), by striking “chapter”
14 and inserting “subchapter”;

15 (14) in section 3518—

16 (A) in subsection (a), by striking “chapter”
17 and inserting “subchapter” each place it ap-
18 pears;

19 (B) in subsection (b), by striking “chapter”
20 and inserting “subchapter”;

21 (C) in subsection (c)(1), by striking “chap-
22 ter” and inserting “subchapter”;

23 (D) in subsection (c)(2), by striking “chap-
24 ter” and inserting “subchapter”;

1 (E) in subsection (d), by striking “chapter”
2 and inserting “subchapter”; and
3 (F) in subsection (e), by striking “chapter”
4 and inserting “subchapter”; and
5 (15) in section 3520, by striking “chapter” and
6 inserting “subchapter”.

7 **SEC. 5. EFFECTIVE DATE.**

8 This Act and the amendments made by this Act shall
9 take effect 30 days after the date of enactment of this Act.